United States Department of State

Privacy Impact Assessment (PIA)

Consular Data Information Transfer System (CDITS)

Version 02.00.00

Last Updated: April 15, 2014

Bureau of Administration

1. Contact Information

Department of State Privacy Coordinator
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

a. Date PIA was completed: April 15, 2014

b. Name of system: Consular Data Information Transfer System

c. System acronym: CDITS

d. IT Asset Baseline (ITAB) number: # 964

e. System description (Briefly describe scope, purpose, and major functions):

CDITS is a communication infrastructure system used to exchange data/information in support of Consular Affairs (CA). CDITS is a General Support System (GSS) composed of several connections that assist with the transfer of visa and passport information via several servers. Only connections that handle personally identifiable information (PII) of U.S. citizens are covered in this PIA. All CDITS communications are encrypted using either hardware encryption, software encryption, or, in some cases, both. The CDITS connections with the following entities are used to transfer passport data:

1. The Bank

   Passport application data is gathered by the commercial bank (referred to as "the Bank"), which processes paper passport applications and the associated application fee. The Bank Lockbox Connection (referred to as the "Lockbox") then transfers this application data to the CDITS servers. Finally, the passport application data is transferred via the State Department intranet in a secure manner to the Travel Document Issuance System (TDIS) to be maintained as a final record.

2. Government Printing Office(GPO)

   CDITS allows the GPO to transmit passport book shipment and product data to Department of State passport agencies and centers over a server-to-server Secure File Transfer Protocol (SFTP) connection. The data transferred via this connection does not contain PII and will not be discussed after section 2.

3. United States Postal Service(USPS)

   CDITS allows passport agencies and centers to transmit a file containing a manifest of used tracking numbers to USPS over the internet. The USPS responds with an audit file indicating receipt of the manifest. Data is encrypted using SSH File Transfer Protocol (SFTP). The data transferred via this connection does not contain PII and will not be discussed after section 2.

4. Drug Enforcement Agency (DEA)

   The Drug Enforcement Agency (DEA) is a Department of Justice (DOJ) entity. CDITS receives a daily file with Visa additions, updates and deletions. The file is transmitted via the Connect: Direct (C: D) server. The FTP server in the DMZ then uses Virtual directories to get the file from the C: D server. The FTP client in OpenNet pulls the file from the DMZ FTP server on a daily basis. IRM controls all of the network equipment at both ends, up to the router at DOJ. This connection goes through the Other Government Agency (OGA) firewall and a DMZ switch.

5. Federal Bureau of Investigation (FBI) National Crime Information Center (NCIC)

   NCIC sends a daily file containing passport information to CDITS via FTP over encrypted network data links. CDITS then routes the file to the State Department namecheck application. The communication between CDITS and the FBI is protected using FIPS 140-2 compliant hardware encryption devices.

f. Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

g. Explanation of modification (if applicable): N/A

h. Date of previous PIA (if applicable): January 19, 2010

3. Characterization of the Information

The system:

- ☐ Does NOT contain PII. If this is the case, you must only complete Section 13.
- ☒ Does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

The elements of PII that are collected by CDITS from each source are as follows:

1. The Bank

   CDITS securely transfers PII passport application and biometric data, including names, sex, date and place of birth, mailing addresses, email addresses, telephone numbers, most recent passport book and card numbers, date and place of any name change, height, hair color, eye color, occupation, name of employer, social security number, and the name, address, and phone number of an emergency contact from the Bank to the CDITS servers and then to the State Department Travel Document Issuance System (TDIS) for further processing.

2. DEA

   CDITS receives a daily file with Visa additions, updates and deletions

3. FBI NCIC

   NCIC sends a daily file containing passport information to CDITS.

b. How is the information collected?

The data collection methods from each source are as follows:

1. The Bank

   The Bank provides lockbox services for passport application processing. Passport applications are received by mail daily. Passport applications are received in paper format and are accompanied with a form of payment covering the processing fee (when applicable) and supporting documentation.

   After the Bank processes the passport application fee, CDITS transfers the passport application information from the Bank to the CDITS servers. No changes to the data are made as a result of the transfer.

2. DEA

   CDITS receives a daily file with Visa additions, updates and deletions

3. FBI NCIC

   NCIC sends a daily electronic file containing passport information to CDITS.

c. Why is the information collected and maintained?

The reasons for collecting data from each source are as follows:

1. The Bank

This information is collected from the Bank, which receives the information from U.S. passport applicants who submit paper passport applications on Form DS-82 for the purpose of transferring the applications electronically to the Department of State for adjudication. Each element of PII collected on Form DS-82 which is captured by CDITS has been determined to be necessary for the determination of an applicant's entitlement to a U.S. passport. This data is not permanently retained by CDITS.

2. DEA

   The VISA data is collected to ensure up to date VISA information.

3. FBI NCIC

   The passport data file is collected to support passport application processing. This data is not permanently retained by CDITS.

d. How will the information be checked for accuracy?

The methods of validating data from each source are as follows:

1. The Bank

Information is not checked for accuracy within CDITS, as it is a transfer mechanism from the Bank to the Department of State. Passport application information is reviewed and checked for accuracy during the passport adjudication process.

2. DEA

Information is not checked for accuracy within CDITS, as it is a transfer mechanism from the DEA to the Department of State.

3. FBI NCIC

Information is not checked for accuracy within CDITS, as it is a transfer mechanism from the FBI to the Department of State's Consular Lookout and Support System (CLASS). Passport application information is validated when it is loaded into CLASS, and is reviewed and checked for accuracy during the passport adjudication process.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 8 U.S.C. 1104 (Powers and Duties of Secretary of State)
- 8 U.S.C. 1401–1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality; Use of U.S. Passports);
- 18 U.S.C. 911, 1001, 1541–1546 (2007) (Crimes and Criminal Procedure);
- 22 U.S.C. 211a–218, 2651a, 2705 (2007); Executive Order 11295, August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports);
- 8 U.S.C. 1185 (2007) (Travel Control of Citizens);

- 22 C.F.R. parts 50 and 51, Citizenship and Naturalization and Passports and Visas;
- Immigration and Nationality Act (INA) of 1952 (P.L. 82-414) and amendments;
- Anti-Drug Abuse Act of 1988 (P.L. 100-690);
- Immigration Act of 1990 (P.L. 101-649);
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208);
- USA PATRIOT Act of 2001 (P. L. 107-56);
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208); and
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

1. The Bank

CDITS is a necessary interface between the Bank and the Department of State's Travel Document Issuance System (TDIS) during the passport application process. CDITS transfers a high volume of passport application data to TDIS regularly. To mitigate privacy risk, strict security and access controls are in place to ensure the confidentiality and integrity of the PII.

The Interconnection Security Agreement (ISA) that is in place specifies requirements for protection of PII transferred via the interconnection between the Bank servers and CDITS servers.

Bank applications processing is performed in accordance with a Service Level Agreement. Applications are processed, batched, scanned, reviewed, and have data entry performed on them. Once all processing is completed, the application data is ready to be retrieved by CDITS.

The Bank to the Department of State data transfer involves CDITS monitoring of specific server directories at the Bank site. These directories are automatically configured to receive the passport image and data files. As the passport application and photo images files become available, CDITS will initiate the file transfer from the Bank server to the CDITS servers. This transfer is secured by National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2 compliant encryption software and hardware.

The data transfer using FIPS 140-2 compliant encryption software that is installed on each of the CDITS and Bank servers. When the data is received by the CDITS servers, it is decrypted and then scanned using Anti Virus software. Finally, the data is sent to TDIS for distribution to the Passport Agencies and Centers via the State

Department intranet. No information is permanently stored on the CDITS network. The data cannot be accessed by CA personnel while in transit.

2. DEA

Risk of modification and disclosure of the PII data is mitigated by the encryption of communications between the DEA and CDITS. Within the State Department intranet, the data is protected by common enterprise security controls.

3. FBI NCIC

Risk of modification and disclosure of the PII data is mitigated by the encryption of communications between the FBI and CDITS. Within the State Department intranet, the data is protected by common enterprise security controls.

4. Uses of the Information

a. Describe all uses of the information.

CDITS routes passport application PII data to other State Department systems for use in processing those applications. The system does not directly perform any processing of the data.

b. What types of methods are used to analyze the data? What new information may be produced?

CDITS does not perform any analysis of the transferred data. No new information is produced.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

CDITS receives a daily electronic file from the FBI/NCIC and transfers the file to Diplomatic Security.

d. Are contractors involved in the uses of the PII?

CDITS is a government owned system. The only users are government personnel. These users are Department of State Bureau of Consular Affairs (CA) System administrators who are allowed to monitor the Bank and CDITS servers. There are no end-users of CDITS. Contractors are involved with the design, development, maintenance, and administration of the system. All System administrators are required to pass annual computer security and privacy training, and to sign non-disclosure and rules of behavior agreements.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Appropriate use of the information is regulated by automated security controls in the CDITS system. CDITS is only used as a data transfer mechanism to and from other CA systems and external agency systems. CDITS does not have any end users.

The State Department installs, operates and manages a state-full inspection firewall and a proxy/application layer firewall to provide port and application proxy layer access controls.

CA operates and manages FIPS 140-2 compliant encryption software on CDITS servers. It is used to encrypt PII data transferred between the Bank servers and CDITS. CA also installs and operates antivirus on the CDITS servers to provide content scanning for virus and malware after data has been decrypted.

5. Retention

a. How long is information retained?

No information is permanently retained by CDITS. Some PII data may be retained temporarily in audit or transaction logs. These logs are only retained online for a variable period of time (typically not more than a few weeks) and then they are archived via off-line media and deleted from on-line servers.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of aging. The privacy risks are mitigated through the controlled access and rules of behavior that govern the users of CDITS throughout the lifetime of the data.

Access to CDITS transaction and audit logs is password-protected and under the direct supervision of the System Manager.

No information is permanently retained by CDITS. PII data may be retained temporarily in audit or transaction logs. The logs can only be accessed by an authorized system administrator and are protected by State Department enterprise security controls. CDITS logs are only retained on-line for a variable period of time (typically not more than a few weeks) and then they are archived via off-line media and deleted from on-line servers.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The only internal organization that has access to CDITS data is the Department of State Bureau of Consular Affairs (CA). Passport application data is processed in CDITS and includes photos, gender, social security numbers, places and dates of

birth, physical mailing and email addresses, and phone numbers. This information is shared with other CA systems.

TDIS interfaces with CDITS via Front End Processor (FEP). The TDIS request is filtered through to CDITS via FEP and the response from CDITS to TDIS is sent back via FEP for the purpose of preventing internal CA major application systems from initiating a direct and formal communication with external systems not on State Department intranet. Information is shared for the purpose of passport application processing.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

For CDITS as a whole, System Administrator access to CDITS servers is protected by passwords, and is under the supervision of system managers. Audit trails track and monitor usage and access. Finally, regularly administered security and privacy training informs authorized system administrators of proper handling procedures.

Specifically, information is transmitted and disclosed as follows:

1. The Bank

CDITS pulls data from the Bank. The data is encrypted in transit. CDITS then transfers this data to TDIS and to other State Department systems via an FTP server over the secure State Department intranet.

2. DEA

Information is transferred from DEA to CDITS via File Transfer Protocol (FTP). The communication between CDITS and the DEA is protected using NIST FIPS 140-2 compliant hardware encryption devices.

3. FBI NCIC

Information is transferred from NCIC to CDITS via File Transfer Protocol (FTP). The communication between CDITS and the FBI is protected using NIST FIPS 140-2 compliant hardware encryption devices.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

The risks associated with sharing PII internally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of PII by personnel can result from social engineering, phishing, abuse of elevated privileges or a general lack of training. To combat the misuse of information, access to CDITS information is controlled by State Department application access controls that are common across the enterprise to reduce and mitigate the risks associated with internal sharing and disclosure. These include, but are not limited to, annual security training, separation of duties, personnel screening, and auditing. In addition, management Control Reports identify actions of authorized system administrators and allows management to review daily activity. User training at the

application level is delivered annually in accordance with internal Department of State regulations.

Vulnerabilities and risks are mitigated through the information system certification process. Recommendations from the National Institute of Standards and Technology (NIST) are strictly adhered to in order to ensure appropriate data transfers and storage methods are applied.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

1. The Bank

   The Bank provides Lockbox services for passport application processing. The Bank receives passport applications by mail daily. Passport applications are received in paper format and are accompanied with a form of payment covering the processing fee (when applicable) and supporting documentation.

   An Interconnection Security Agreement (ISA) helps to mitigate privacy risks for the interconnection between the Bank's Lockbox servers and CA's Consular Data Information Transfer System (CDITS) servers.

   CDITS then sends the passport data, via State Department secure intranet, to TDIS for forwarding to the passport agencies and centers.

2. DEA

   VISA related PII is transferred from DEA to CDITS for the purpose of VISA application processing.

3. FBI NCIC

   Passport related PII is transferred from NCIC to CDITS for the purpose of passport application processing.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

1. The Bank

   CDITS passport data is collected by the Bank. Bank administrators prepare the photo and biometric data for CDITS server pick-up. There is a Memorandum of Understanding (MOU) and an Information Security Agreement (ISA) in place that provides the requirement for sharing of the information. CA administrators monitor the specific directories at the Bank site that contain the passport image and data files. As the passport application and photo image files become available, CDITS will initiate the file transfer from the Bank server to the CDITS servers.

2. DEA

   VISA related PII is transferred from DEA to CDITS for the purpose of VISA application processing.

3. FBI NCIC

   Information is transferred from NCIC to CDITS via File Transfer Protocol (FTP). The communication between CDITS and the FBI is protected using NIST FIPS 140-2 compliant hardware encryption devices.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The primary risk is misuse by external agencies' employees and contractors. Misuse may result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress for applicants whose PII is compromised. In addition to administrative burdens, data compromises may escalate to financial loss; loss of public reputation and public confidence; and civil liability for the Department of State and other agencies.

To appropriately safeguard the information, numerous management, operational, and technical security controls are in place in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST). Access control lists for external sharing, which define who can access the system and at what privilege level, are regularly reviewed, and inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. An audit trail provides a record of all functions authorized users perform--or may attempt to perform.

There are slight variations in how privacy risks are mitigated from external agency to external agency, which are specifically discussed below:

1. The Bank

   The risks of unauthorized disclosure or modification of PII Passport data are mitigated as follows:

   - The Bank processes passport data in accordance with State Department security requirements for processing of PII. Compliance with these requirements is enforced by the ISA between State and the Bank.
   - All data transfers between CDITS and the Bank are encrypted using the FIPS 140-2 compliant software installed on the Bank and CDITS servers.

2. DEA

   Information is transferred from DEA to CDITS via File Transfer Protocol (FTP). The communication between CDITS and the DEA is protected using NIST FIPS 140-2 compliant hardware encryption devices.

3. FBI NCIC

   Information is transferred from NCIC to CDITS via File Transfer Protocol (FTP). The communication between CDITS and the FBI is protected using NIST FIPS 140-2 compliant hardware encryption devices.

8. Notice

The system:

☒ Contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

• Passport Records, State-26

☐ Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Notice is provided at the point of collection during the application process. The data is collected from the applicant on the paper passport application before any of the data is processed by CDITS. Additionally, notice of the routine uses of the information is provided in the System of Record Notice (SORN) for Passport Records, STATE-26.

For data supplied by the FBI on wanted persons, the notice may not be provided and the individual may not be voluntarily providing the data.

b. Do individuals have the opportunity and/or right to decline to provide information?

No. However, the passport applicant voluntarily provides the information when they fill out the paper passport application point of collection during the application process. The data is collected from the applicant before any of the data is processed by CDITS.

Data provided by the FBI may be collected from sources other than the applicant so there would be no opportunity for the individual to decline to provide information.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No. Once information is collected by the passport agency, an individual does not have the right to consent to limited, special, and/or specific uses of information.

For information provided by the FBI, an individual does not have the right to consent to limited, special, and/or specific uses of information.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

For passport application data, the notice provided is adequate and reasonable, and is provided at the collection points of information (i.e. the passport application forms). No passport application information is collected from individuals without their knowledge.

All information provided by external agencies is collected outside of State Department control.

In all cases, the risks associated with individuals being unaware of information collection by the State Department are mitigated by restrictions on access to CDITS. Access to PII that is transmitted by CDITS is restricted to cleared, authorized users.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Not applicable. CDITS does not permanently store any PII so there is nothing for an individual to request access to.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

There is minimal risk associated with Notification and Redress imposed by CDITS since it neither collects PII directly from users nor permanently stores any such information. The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's stated purposes and uses and its applicable legal requirements. Therefore, this category of privacy risk is appropriately mitigated in CDITS.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Only Department of State administrators have access to CDITS servers and network devices for the purpose of carrying out their official duties, which are limited to monitoring and auditing application processes. Activities that will be recorded include: event type, date and time of event, server identification, success or failure of administrator access attempts, and security actions.

The State Department maintains 24x7 Network Operations Centers that are responsible for monitoring of firewall, scanning, and encryption equipment in the network transmission path of centrally managed and automated servers. Tracking

events identified are not captured entirely by a single protection device but by a combination of all of the devices in the transmission path. Monitoring events outside the network boundaries on Bank Lockbox servers, including the use and management of FIPS 140-2 compliant encryption products and antivirus content level scanning, are the responsibility of CA. To meet this requirement, CDITS servers and Bank Lockbox servers are configured to comply with the all applicable Diplomatic Security configuration guide policies on auditing and in accordance with 12 FAM 652.3-4 Audit.

b. What privacy orientation or training for the system is provided authorized users?

Users internal to the Department must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain the access, users must complete annual refresher training.

Internal based users must read and accept the Computer Fraud and Abuse Act Notice and Privacy Act Notice that outline the expected use of these systems and how they are subject to monitoring prior to being granted access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. An audit trail provides a record of all functions authorized users perform or may attempt to perform. The trainings and controls described above are adequate in their protection of CDITS information from unauthorized access and use. As a result, the residual risk is judged to be acceptable.

11. Technologies

a. What technologies are used in the system that involves privacy risk?

CDITS uses secure networks in addition to FIPS 140-2 compliant encryption software between servers to transfer information. These technologies do not elevate privacy risk. All known vulnerabilities identified by the industry related to CDITS technologies have been mitigated. During the regular monitoring process, new vulnerabilities are identified and fixed.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Since CDITS does not use any technology known to elevate privacy risk, standard robust safeguards are determined to be satisfactory in this general support system (GSS). Rigorous ongoing monitoring, testing, and evaluation of security controls are conducted to ensure that the safeguards continue to fully function.

12. Security

a. What is the security assessment and accreditation (A&A) status of the system?

The Department of State operates CDITS in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security management Act (FISMA) of 2002, the triennial assessment and authorization of this system was completed in March 2014. This document was updated as part of the triennial reauthorization of the system.